

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-102020

(43)Date of publication of application : 15.04.1997

(51)Int.Cl.

G06K 17/00

G06F 9/06

(21)Application number : 07-257999

(71)Applicant : TOPPAN PRINTING CO LTD

(22)Date of filing : 04.10.1995

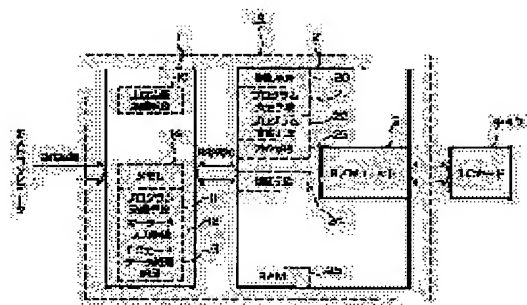
(72)Inventor : HIRANO SEIJI
MATSUMURA SHUICHI
YURA AKIYUKI

(54) IC CARD TERMINAL

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an IC card terminal high in security and capable of easily altering a processing program.

SOLUTION: When the processing of an IC card authentication program NP starts, whether an IC card 4 is inserted into an R/W unit 3 or not is judged. Then, the activation of the I/C card 4 is detected based on ATR information. When the IC card 4 is an authenticating card 4', the propriety of the IC card 4, that of the IC card terminal A and that of a system are recognized. When they are judged to be impropriety in an authentication processing, an error flag is stored in RAM 25. When the IC card authentication processing is ended, the IC card 4 is discharged from the R/W unit 3 and a new IC card processing program IPQ is loaded.



LEGAL STATUS

[Date of request for examination] 09.09.2002

[Date of sending the examiner's decision of rejection] 05.07.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-102020

(43) 公開日 平成9年(1997)4月15日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00			G 0 6 K 17/00	E
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 K

審査請求 未請求 請求項の数5 O L (全 9 頁)

(21) 出願番号 特願平7-257999

(22) 出願日 平成7年(1995)10月4日

(71) 出願人 000003193
凸版印刷株式会社
東京都台東区台東1丁目5番1号

(72) 発明者 平野 誠治
東京都台東区台東1丁目5番1号 凸版印刷株式会社内

(72) 発明者 松村 秀一
東京都台東区台東1丁目5番1号 凸版印刷株式会社内

(72) 発明者 由良 彰之
東京都台東区台東1丁目5番1号 凸版印刷株式会社内

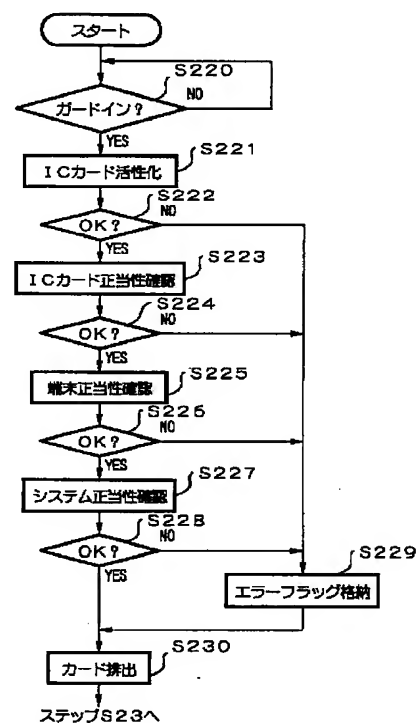
(74) 代理人 弁理士 川▲崎▼ 研二 (外1名)

(54) 【発明の名称】 ICカード端末

(57) 【要約】

【課題】 セキュリティが高く、処理プログラムの変更が容易なICカード端末を提供する。

【解決手段】 ICカード認証プログラムNPの処理が開始すると、まず、R/WユニットにICカード4が挿入されているか否かを判定し(S220)、その後、ICカード4の活性化をATR情報に基づいて検出する(S221)。ICカード4が認証用カード4であるならば、ICカード4の正当性、ICカード端末Aの正当性、システムの正当性を確認する(S223~S228)。上記認証処理で不当と判定された場合には、エラーフラグをRAM25に格納する(S229)。こうして、ICカード認証処理が終了すると、ICカード4をR/Wユニット3から排出し(S230)、新たなICカード処理プログラムIPQをローディングする。



(2)

1

【特許請求の範囲】

【請求項1】 データの読出または書込のうち少なくとも一方をＩＣカードに対して行うＩＣカード端末において、

前記ＩＣカードに対応した処理プログラムを記憶する不揮発性の記憶手段と、

この処理プログラムを書き換える際、書換の正当性を認証する認証手段と、

この認証手段によって正当性が認証された場合に前記記憶手段に格納されている前記処理プログラムを書き換える書換手段と、

前記ＩＣカードに対してデータの読出または書込のうち少なくとも一方を行うインターフェース手段と、

前記処理プログラムに基づいて、前記インターフェース手段を制御する制御手段とを備えたことを特徴とするＩＣカード端末。

【請求項2】 前記認証手段は、認証用ＩＣカードの正当性を認証することを特徴とする請求項1に記載のＩＣカード端末。

【請求項3】 前記認証手段は、認証用ＩＣカードが前記ＩＣカード端末の正当性を認証した認証情報に基づいて、書換の正当性を認証することを特徴とする請求項1に記載のＩＣカード端末。

【請求項4】 前記認証手段は、暗号関数または復号関数を用いて、書換の正当性を認証することを特徴とする請求項1乃至3のいずれか1項に記載のＩＣカード端末。

【請求項5】 前記記憶手段、前記認証手段、前記書換手段、および前記制御手段を有する演算処理装置を備えたことを特徴とする請求項1乃至4のいずれか1項に記載のＩＣカード端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ＩＣカード端末に関するものであり、特に、セキュリティが高く、また新たなＩＣカードにも対応できるシステムを構築するのに好適である。

【0002】

【従来の技術】ＩＣカードは、内部に半導体メモリを有し、そこに大量の情報を記憶できしかも携帯に便利であることから、その利用分野は急速に拡大されつつある。これに伴い、用途に応じたＩＣカードが各種開発されつつある。これらのＩＣカードにあつては、そのクロック周波数や通信プロトコルが相違するのが通常である。したがって、新たなＩＣカードが開発されると、従来のＩＣカード端末では対応できず、その制御プログラムを変更する必要がある。

【0003】

【発明が解決しようとする課題】ところで、この制御プログラムは、ＰＲＯＭやＣＰＵ内部のマスキングＲＯＭに格

2

納されているか、あるいは、電話回線等の通信回線を介してＩＣカード端末内のメモリにローディングされる。

【0004】しかし、ＰＲＯＭに制御プログラムを格納したのでは、ＰＲＯＭ自体が盗難された場合、制御プログラムを容易に読み出されてしまう。また、制御プログラムを変更するにはＰＲＯＭやＣＰＵを交換する必要がある、不便である。一方、制御プログラムを通信回線を介して配信する場合にあつては、第3者が通信回線を介してＩＣカード端末にアクセスする虞がある。このため、制御プログラムの偽造、改変等の可能性があり、セキュリティが低いという問題があつた。

【0005】本発明は上述した事情に鑑みてなされたものであり、セキュリティが高く、かつ、制御プログラムの変更が容易なＩＣカード端末を提供することを目的とする。

【0006】

【課題を解決するための手段】上記課題を解決するため請求項1に記載のこの発明にあつては、データの読出または書込のうち少なくとも一方をＩＣカードに対して行うＩＣカード端末において、前記ＩＣカードに対応した処理プログラムを記憶する不揮発性の記憶手段と、この処理プログラムを書き換える際、書換の正当性を認証する認証手段と、この認証手段によって正当性が認証された場合に前記記憶手段に格納されている前記処理プログラムを書き換える書換手段と、前記ＩＣカードに対してデータの読出または書込のうち少なくとも一方を行うインターフェース手段と、前記処理プログラムに基づいて、前記インターフェース手段を制御する制御手段とを備えたことを特徴とする。

【0007】また、請求項2に記載のこの発明にあつては、前記認証手段は、認証用ＩＣカードの正当性を認証することを特徴とする。また、請求項3に記載のこの発明にあつては、前記認証手段は、認証用ＩＣカードが前記ＩＣカード端末の正当性を認証した認証情報に基づいて、書換の正当性を認証することを特徴とする。

【0008】また、請求項4に記載のこの発明にあつては、前記認証手段は、暗号関数または復号関数を用いて、書換の正当性を認証することを特徴とする。また、請求項5に記載のこの発明にあつては、前記記憶手段、前記認証手段、前記書換手段、および前記制御手段を有する演算処理装置を備えたことを特徴とする。

【0009】

【発明の実施の形態】

1. 実施形態の構成

以下、図面を参照してこの発明の実施形態の構成について説明する。図1はこの発明に係るＩＣカード端末が適用されるＩＣカードシステムの一実施形態のブロック図である。図1において、1はパーソナルコンピュータであり、通信回線を介して図示せぬホストコンピュータと接続されている。2はＩＦＤ回路であり、パーソナルコ

(3)

3

ンピュータ1と接続され、パーソナルコンピュータ1から送信される制御プログラムSPを受信し、この制御プログラムSPに基づいて、データの書込読出を行う。3はR/Wユニットであり、ICカード4からデータを読み出し、また、データの書き込む。AはICカード端末であり、上記したパーソナルコンピュータ1、IFD回路2およびR/Wユニット3から構成される。なお、4は認証用カードであり、プログラムを書き換える際に、その正当性を認証するために用いられる。

【0010】次に、パーソナルコンピュータ1は、以下の部分により構成される。10は上位装置通信手段であり、ホストコンピュータとのインタフェースであり、制御プログラムSPの受信や各種のデータ通信を行う。また、11はプログラム送信手段であり、IFD回路2に対して、制御プログラムSPをRS232Cの形式で送信する。また、12はキーボードで構成されるキーデータ入力手段であり、これにより、操作指示が入力される。また、13はICカードデータ処理手段であり、ICカード4に格納すべきデータを暗号化し、またICカード4から読み出したデータを復号化する。

【0011】また、IFD回路2は以下の部分により構成される。20は制御手段であり、IFD回路2の動作全体を制御する。21はプログラム受信手段であり、パーソナルコンピュータ1から送信される制御プログラムSPを受信する。22はプログラム書換手段であり、制御プログラムSPの一部または全部の書換を行う。23はフラッシュメモリであり、書換可能で揮発性である。フラッシュメモリ23には、制御プログラムSPが格納される。24は認証手段であり、制御プログラムSPの一部書換に際して、書換の正当性を認証する。25はRAMであり、制御手段20の作業領域として機能する。

【0012】ここで、フラッシュメモリ23に格納される制御プログラムSPについて、図2を用いて説明する。図2はフラッシュメモリ23のメモリマップである。同図示すように制御プログラムSPは、メインプログラムMP、RAM転送プログラムRP、ICカード処理プログラムNP、書換プログラムKPおよびICカード処理プログラムIPから構成される。

【0013】まず、第1ブロックB1にはメインプログラムMPが格納される。このメインプログラムMPは、IFD回路2をデータ読出・書込可能な状態にすると共に、所定の場合に書換プログラムKPを実行する。

【0014】また、第2ブロックB2には、RAM転送プログラムRP、ICカード認証プログラムNPおよび書換プログラムKPが格納される。RAM転送プログラムRPは、所定のブロックに格納されているプログラムをRAM25に転送するためのプログラムである。また、ICカード認証プログラムNPは、ICカードを用いて、ICカードの正当性、端末の正当性およびシステ

4

ムの正当性を確認するためのプログラムである。また、書換プログラムKPは、第3ブロックB3に格納されているプログラムを書き換えるためのプログラムである。

【0015】また、第3ブロックB3には、ICカード処理プログラムIPが格納される。ICカード処理プログラムは、パーソナルコンピュータ1からのコマンドを受信し、そのコマンドの処理を行うためのプログラムである。なお、第1、第2ブロックB1、B2に格納されたプログラムは、動作処理の基本プログラムであるため、固定であるが、第3ブロックB3に格納されたプログラムは、対象とするICカードのバージョンアップやシステム変更に対応できるように、書換可能である。

【0016】次に、IFD回路2の具体的な構成を図3を参照して説明する。図3はIFD回路の回路図である。同図において、200はCPUであり、上記した制御手段20、プログラム書換手段22、フラッシュメモリ23、認証手段24およびRAM25として機能する。この例では、CPU200にH8/538F（日立製作所）を用いている。

【0017】CPU200において、XTAL、EXTALはクロック入力端子であり、そこには4.9152MHzで発振する水晶振動子201が接続される。また、MD0、MD1、MD2は、動作モード端子であり、これらの接続状態によって、CPU200の動作モードが設定される。例えば、動作モード端子MD0、MD1、MD2に5Vが供給される場合には、通常モードとして動作する。通常モードにあっては、RAM25に格納されているプログラムを実行したり、フラッシュメモリ23に格納されているプログラムの一部を書き換える。一方、動作モード端子MD0、MD1に5Vが供給されると共に動作モード端子MD2に1.2Vが供給される場合には、ブートモードとして動作する。ブートモードでは、CPU200の内部にあるフラッシュメモリ23に格納されているプログラムが全て消去され、プログラムの書込が再度行われる。

【0018】また、Vppは、フラッシュメモリ23の消去用電源供給端子であり、リセット出力端子を兼ねる。RESは、リセット端子であり、そこにローレベルが供給されるとCPU200の動作は初期化される。なお、端子Vppに1.2Vが供給されると、フラッシュメモリコントロールレジスタの第7ビットにフラッグが発生するよう構成されている。

【0019】また、P60～P64は第6ポートの入出力端子、P72～P77は第7ポートの入出力端子である。このうち、端子P72、P73、P76、P77は、インターフェース手段210（MAX232）に接続されており、コネクタ211を介してパーソナルコンピュータ1とデータの交換を行う。具体的には、端子P72はシリアルデータを送信し、端子P73はシリアルデータを受信し、端子P76、P77はクロック信号を入出力する。なお、インターフェース手段210はシリアルデータとRS232C形式データとを相互に変換

(4)

5

するものであり、上記したプログラム受信手段21として機能する。

【0020】また、端子P60～P64、P74、P75は、R/Wユニット3の各端子と接続される。すなわち、端子P61はリセット端子RESETと、端子P74、P75はデータの入出力を行うデータ入出力端子I/Oと、端子P62は電源端子Vccと、端子P63はカード入力信号を出力する端子CIと、端子P64はカード出力信号を入力する端子C0と、端子60はNAND回路を介してクロック信号を入力する端子CLKと接続される。

【0021】2. 実施形態の動作

以下、図面を参照してこの発明の実施形態の動作について説明する。この実施形態の動作は、ブートモード動作、実行動作、書換動作に大別される。以下、場合を分ち説明する。

【0022】2-1 ブートモード動作

ブートモードでは、CPU200を制御する制御プログラムSPを初期書込する。以下、図4を参照してブートモード動作を説明する。

【0023】まず、スイッチSW3をON状態にしてリセット端子RESをローレベルにすると（ステップS1）、CPU200の動作が初期化される。そして、スイッチSW1、SW2をON状態にすると（ステップS2）、動作モード端子MD2と端子Vppには12Vが供給される。この後、スイッチSW3をOFF状態にしてリセット端子RESをハイレベルにすると（ステップS3）、CPU200は、ブートモードに遷移し、フラッシュメモリ23への書込データを受け付ける状態となる。

【0024】次に、ステップS4に進み、パーソナルコンピュータ1から制御プログラムSPがプログラム送信手段11（図1参照）を用いて送信されると、これがコネクタ211とインターフェース手段210とを介してCPU200に供給され、その内部にあるフラッシュメモリ23の各ブロックB1～B3に制御プログラムSPが書き込まれる。

【0025】こうして、フラッシュメモリ23には、第1ブロックB1にメインプログラムMPが、第2ブロックB2にRAM転送プログラムRP、ICカード認証プログラムNPおよび書換プログラムKPが、第3ブロックB3にICカード処理プログラムIPがそれぞれ書き込まれる。

【0026】2-2 実行動作

実行動作では、設定される条件に応じて、ICカード処理プログラムモードとユーザープログラムモードとを選択する。ICカード処理プログラムモードではICカード処理プログラムNPを実行し、ユーザープログラムモードでは書換プログラムKPを実行する。以下、図5を参照しつつ、実行動作を説明する。

【0027】まず、スイッチSW3をON状態にすると、リセット端子RESがローレベルとなり（ステップS

6

10）、CPU200の動作が初期化される。そして、スイッチSW1をOFF状態にすると（ステップS11）、動作モード端子MD2の電圧は5Vとなり、CPU200は通常モードに遷移する。この後、リセット端子RESをハイレベルにすると（ステップS12）、CPU200は、フラッシュメモリ23に格納されているメインプログラムMPをRAM25に転送し、これを実行する。

【0028】メインプログラムMPの処理が開始すると、まず、端子Vppの電圧が12Vであるか否かが判定される（ステップS13）。具体的には、フラッシュメモリコントロールレジスタの第7ビットにフラグが存在するか否かによって、端子Vppに12Vが供給されているか否かが判定される。

【0029】スイッチSW2がON状態であるならば、端子Vppの電圧が12Vとなり、ステップS13で「YES」と判定され、ステップS14に進んで、ユーザープログラムモードに遷移する。ユーザープログラムモードとは、フラッシュメモリ23に格納されているICカード処理プログラムIPを書き換えるモードである。一方、スイッチSW2がOFF状態であるならば、端子Vppの電圧は5Vとなり、ステップS13で「NO」と判定され、ステップS15に進んで、ICカード処理モードに遷移する。以下、ユーザープログラムモードとICカード処理モードとを場合を分ち詳述する。

【0030】2-2-1 ユーザープログラムモード動作

図6はユーザープログラムモードのフローチャートである。同図において、まず、フラッシュメモリ23から、その第2ブロックB2に格納されているICカード認証プログラムNPと書換プログラムKPとをRAM25に転送する（ステップS20）。この転送が終了すると、CPU200はRAM25に格納されたICカード認証プログラムNPを実行し、その後、書換プログラムKPを実行する（S21）。

【0031】ステップS22では、ICカード認証プログラムNPを実行する。この動作を図7に示すICカード認証プログラムNPのフローチャートを用いて説明する。ICカード認証プログラムNPの処理が開始すると、まず、R/WユニットにICカード4が挿入されているか否かを判定する（ステップS220）。具体的には、端子P63に供給されるカード入力信号の有無をCPU200で検出する。ここで、ICカード4が挿入されていないければ、「NO」を選択し、ICカード4が挿入されるまでこの判定を繰り返す。

【0032】そして、ICカード4が挿入されると、「YES」を選択して、ICカード4の活性化を検出する（ステップS221）。具体的には、図3に示す端子60をハイレベルにしてゲートを開きクロック信号を端子CLKに供給する。また、端子P62から電源を電源端子Vcc

(5)

7

に供給した後、端子P61をハイレベルにしてリセット信号をリセット端子RESETに供給する。この後、ICカード4の種別を表すATR情報がR/Wユニット3から出力されると、端子P74, P75に供給されるATR情報を検出する。そして、ATR情報が認証用カード4'を表しているか否かを判定し（ステップS222）、ICカード4が認証用カード4'でない場合には、「NO」を選択し、ステップS229に進んで、エラーフラッグをRAM25に格納し、ICカード4を排出する（ステップS230）。これにより、認証用カード4'を用いなければ、ICカード処理プログラムIPの書換を行うことができない。

【0033】ICカード4が認証用カード4'であるならば、「YES」を選択しステップS223に進み、ICカード4の正当性を確認する。この動作シーケンスを図8を用いて説明する。まず、ICカード端末A内のCPU200において、乱数Aを発生し、これにキーIDを付加してICカード4に送信する。キーIDは、ICカード4に格納されている各種のIDの中から所定のIDを特定するための情報である。この場合のキーIDはカードIDを指示する。

【0034】この後、ICカード端末A内のCPU200は、カードIDを鍵K1として用い、乱数Aを暗号化して乱数Bを生成する。ここで暗号関数をEとすれば、乱数Bは、次式で表される。

$$B = E(A, K1)$$

【0035】一方、ICカード4にあっては、キーIDと乱数Aを受信すると、内部のメモリをアクセスし、キーIDに基づいてカードIDを読み出す。そして、このカードIDを鍵K1'として用い、乱数Aを暗号化して乱数B'を生成する。ここで用いられる暗号関数はEであり、ICカード端末A内で用いられる暗号関数と同一である。乱数B'は、次式で表される。

$$B' = E(A, K1')$$

【0036】この後、乱数B'がICカード4からICカード端末Aに送信されると、CPU200は乱数Bと乱数B'が一致するか否かを判定する。両者が一致するのは、同一の暗号関数、同一の鍵を用いて暗号化した場合であるから、この場合にはICカード4は正当であると判定される。一方、乱数Bと乱数B'が不一致であれば、ICカード4は不当であると判定される。

【0037】このようにして、ICカード4の正当性がICカード端末Aによって確認され、図7に示すステップS224に進む。そして、ICカード4が不当な場合には、エラーフラッグをRAM25に格納し（ステップS229）、ICカード4をR/Wユニット3から排出する（ステップS230）。一方、ICカード4が正当である場合には、ICカード端末Aの正当性を確認する（ステップS225）。この動作シーケンスを図9を用いて説明する。

8

【0038】まず、ICカード端末A内のCPU200が乱数要求を発生し、これをICカード4に送信すると、ICカード4の内部で乱数Aを発生し、乱数AをICカード端末Aに返信する。これを受けたICカード端末Aは、端末IDを鍵K2として用い、乱数Aを暗号化して乱数Bを生成する。ここで暗号関数をEとすれば、乱数Bは、次式で表される。

$$B = E(A, K2)$$

【0039】この後、CPU200は、乱数BにキーIDを付加してICカード4に送信する。この場合のキーIDは端末IDを特定する。乱数BとキーIDをICカード4が受信すると、ICカード4は内部のメモリをアクセスし、キーIDに基づいて端末IDを読み出す。そして、この端末IDを鍵K2'として用い、乱数Bを復号化して乱数A'を生成する。ここで用いられる復号関数はDであり、ICカード端末A内で用いられる暗号関数Eと相補的な関係にある。乱数A'は、次式で表される。

$$A' = D(B, K2')$$

【0040】この後、ICカード4は乱数Aと乱数A'が一致するか否かを判定する。両者が一致するのは、暗号関数と復号関数が相補的な関係にあり、同一の鍵を用いて暗号化・復号化した場合である。この場合にあっては、ICカード4は、ICカード端末Aが正当であると判定し、正常を表すステータスSJをICカード端末Aに送信する。一方、乱数Bと乱数B'が不一致であれば、ICカード4は、ICカード端末Aが不当であると判定し、異常を表すステータスSJをICカード端末Aに送信する。

【0041】このようにして、ICカード端末Aの正当性がICカード4によって確認され、図7に示すステップS226に進む。ここで、CPU200は、ステータスSJが正常か否かを判定し、異常あれば「NO」を選択して、エラーフラッグをRAM25に格納し、ICカード4をR/Wユニット3から排出する（ステップS230）。

【0042】一方、ステータスSJが正常であれば「YES」を選択し、システムの正当性を確認する（ステップS228）。具体的には、作業者がキーボードを操作して暗証番号やシステムキーを入力すると、CPU200がその正当性を確認する。暗証番号やシステムキーが不当であれば「NO」を選択して、エラーフラッグをRAM25に格納し、ICカード4をR/Wユニット3から排出する（ステップS230）。一方、暗証番号やシステムキーが正当であれば、認証動作を終了し、ICカード4をR/Wユニット3から排出する（ステップS230）。

【0043】こうして、ICカード認証処理が終了すると、図6に示すステップS23に進んで、プログラムの書換を行うか否かを判定する。具体的には、RAM25

50

(6)

9

にエラーフラッグが格納されているか否かによって判定し、エラーフラッグが格納されていれば「NO」を選択し、ステップS22に戻る。一方、エラーフラッグが格納されていなければ「YES」を選択し、ステップS25に進む。

【0044】ステップS25では、フラッシュメモリ23の第3ブロックB3に格納されているICカード処理プログラムIPを消去する。この後、パーソナルコンピュータ1が、新たなICカード処理プログラムIPQを送信すると、これを受信してRAM25に一旦格納する（ステップS25）。この例にあっては、通信フォーマットにモトローラSフォーマットを用いる。このモトローラSフォーマットでは、送信の際に付加したアドレスが、通信データを格納すべきフラッシュメモリ23上の領域を指示する。

【0045】この後、RAM25から当該ブロックにICカード処理プログラムIPQを転送し、その書込を行う（ステップS26）。書込終了後、ICカード処理プログラムIPQのベリファイを行う（ステップS27）。ただし、RAM25の容量には制限があるので、上記ステップS25～S27の処理は、所定バイト単位で行われる。このため、ステップS28では、ICカード処理プログラムIPQについて全処理が終了したか否かを判定する。未処理である場合には、「NO」と判定され、ステップS25からステップS28までの処理を繰り返す。そして、全処理が終了すると、「YES」と判定され、ステップS29に進んで、スイッチSW2をOFF状態にする。これにより、端子Vppが5Vとなり、ステップS14のユーザプログラムモード（図5参照）が終了し、ICカード処理プログラムが変更される。

【0046】2-2-2 ICカード処理モード動作
次に、ICカード処理モード動作を図10を参照しつつ説明する。図10はICカード処理モードのフローチャートである。まず、パーソナルコンピュータ1から送信されるコマンドをIFD回路2が受信すると（ステップS30）、そのコマンドに基づいてICカードコマンド処理を行うか否かを判定する（ステップS31）。具体的には、コマンドの先頭コードを参照する。この例にあっては、先頭コードが2Ehの場合が、ICカードコマンド処理を指示する。したがって、先頭コードが2Ehであれば「YES」を選択し、ICカードコマンド処理を実行する（ステップS32）。

【0047】ICカードコマンド処理ではICカード4に対してデータ読出・書込を行う。例えば、受信したコマンドがデータ読出を指示する場合にあっては、アプリケーションで使用するファイルをICカード4にアクセスして選択し、鍵の照合を行い、この後、データをICカード4からデータを読み出す。なお、データ読出に際して、キーボードからパスワードを入力し、鍵の照合を

10

行っても良い。

【0048】また、受信したコマンドがデータ書込を指示する場合にあっては、アプリケーションで使用するファイルをICカード4にアクセスして選択し、鍵の照合を行い、この後、データをICカード4へデータを書き込む。なお、データ書込に際して、キーボードからパスワードを入力し、鍵の照合を行っても良い。

【0049】一方、コマンドの先頭コードが2Ehでなく、ICカードコマンド処理を指示しない場合にあっては、ステップS31で「NO」と判定され、ステップS33に進んで、R/Wコマンド処理が実行される。ここでは、パーソナルコンピュータ1から受信したコマンドに基づいて、カード排出やカード挿入待等の処理を行う。

【0050】こうして、ICカードコマンド処理（ステップS32）またはR/W制御コマンド処理（ステップS33）が終了すると、その処理結果をパーソナルコンピュータ1に対して出力する（ステップS34）。これを受けてパーソナルコンピュータ1は、新たな指示をIFD回路2に対して出力するか、処理を終了するかを判断する。新たな指示を出す場合にはステップS30に戻り、ステップS30～ステップS34の処理を繰り返す。

【0051】以上説明したようにこの実施形態によれば、CPU200の内部にあるフラッシュメモリ23にICカード処理プログラムIPを格納するので、第3者はICカード処理プログラムIPを容易に読み出すことができない。また、ICカード処理プログラムIPは、書換の正当性を認証した後でなければ、書き換えないので、セキュリティを向上させることができる。また、新たなICカード処理プログラムIPQをホストコンピュータから送信し、オンボード上で書換を行うので、PR-OMやCPUの交換が不要となり、ICカード処理プログラムIPの変更が容易となる。

【0052】3. 変形例

本発明は上述した実施形態に限定されるものでなく、例えば以下のように種々の変形が可能である。

【0053】①上記実施形態において、ブートモード時の書込は、パーソナルコンピュータ1から制御プログラムSPを受信して書き込んでいたが、ROMライタを用いて書き込んでも良い。

【0054】②上記実施形態において、ICカード処理プログラムIPの書換には、ICカードの正当性確認（ステップS223）、端末の正当性確認（ステップS225）およびシステム正当性確認（ステップS227）を全て行ったが、このうちのいずれか1つ、または、これらを適宜組み合わせで行っても良い。また、ICカードの正当性確認と端末の正当性確認とを同時に行う相互認証であっても良い。

【0055】③上記実施形態において、認証処理に用い

50

(7)

11

る暗号関数・復号関数は(図8, 9参照)、例えば、DES, FEALの他、配送鍵方式の一方式であるRSAであっても良い。

【0056】④上記実施形態において、ICカード4は、マルチアプリケーションに対応するものであっても良い。すなわち、このICカードは、複数の通信プロトコルや複数のコマンドコード、パラメータに対応する。この種のICカードにあっては、ファイル選択と鍵照合が同一コマンドであり、これを実行した後、データを読み出すコマンドを実行すれば、所定のデータを読み出せるICカードも存在する。このため、上述したICカードコマンド処理において(図10 ステップS32参照)、コマンドをそのまま送信するようにしても良い。

【0057】⑤上記実施形態において、新たなICカード処理プログラムIPQを認証用カード4'に格納し、書換の正当性が認証されたならば、そこからICカード処理プログラムIPQをICカード端末Aにローディングしても良い。

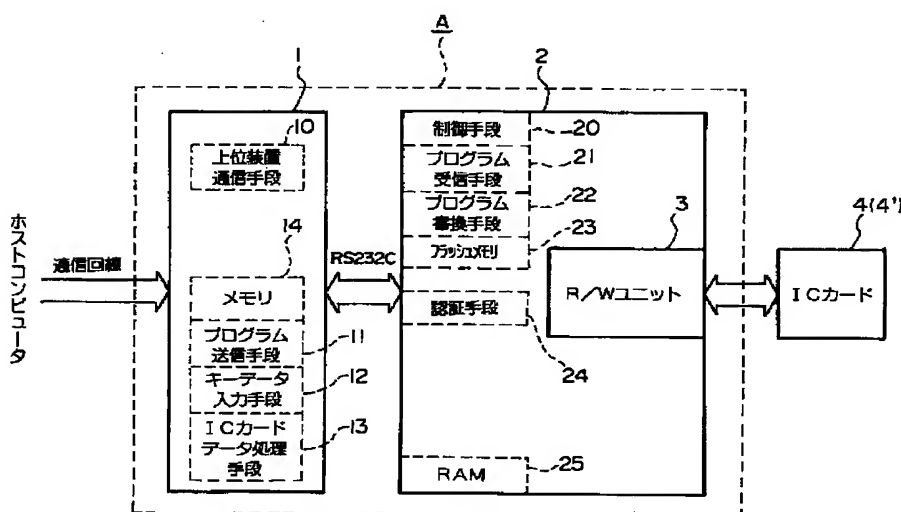
【0058】

【発明の効果】以上説明したように、請求項1乃至5に記載した発明によれば、認証手段で書換の正当性が認証された場合に処理プログラムを書き換えるので、セキュリティを向上させることができる。特に、請求項5に記載の発明にあっては、演算処理装置の内部に認証手段と記憶手段を備えるから、ICカード端末が盗難されても、処理プログラムを読み出すことができないため、セキュリティを大幅に向上させることができる。また、処理プログラムは書換可能であるため、新たなICカードが開発された場合にも迅速に対応することができる。

【図面の簡単な説明】

【図1】 この発明の一実施形態のブロック図である。

【図1】



12

【図2】 同実施形態におけるフラッシュメモリのメモリマップである。

【図3】 同実施形態における各ICカードの通信フォーマットを示す説明図である。

【図4】 同実施形態に用いられるIFD回路の回路図である。

【図5】 同実施形態におけるブートモード動作を説明するためのフローチャートである。

【図6】 同実施形態における実行動作を説明するためのフローチャートである。

【図7】 同実施形態におけるICカード認証プログラムのフローチャートである。

【図8】 この発明の他の実施形態を説明するためのフローチャートである。

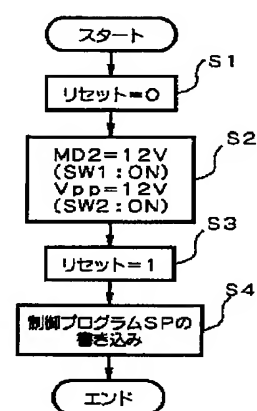
【図9】 一のICカードに対応したATR情報のタイミングチャートである。

【図10】 他のICカードに対応したATR情報のタイミングチャートである。

【符号の説明】

- 4 ICカード
- 4' 認証用カード
- 3 R/Wユニット (インターフェース手段)
- 22 プログラム書換手段 (書換手段)
- 23 フラッシュメモリ (記憶手段)
- 24 認証手段
- 200 CPU (制御手段, 書換手段, 認証手段, 記憶手段, 演算処理装置)
- A ICカード端末
- IP ICカード処理プログラム (処理プログラム)
- SJ ステータス (認証情報)

【図4】

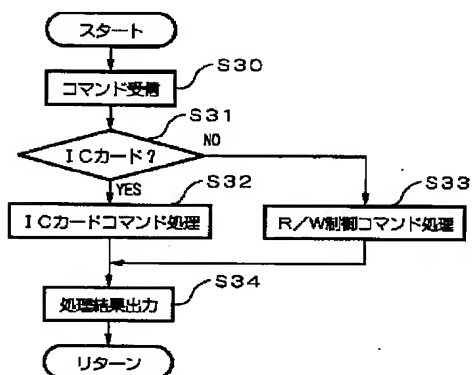


(8)

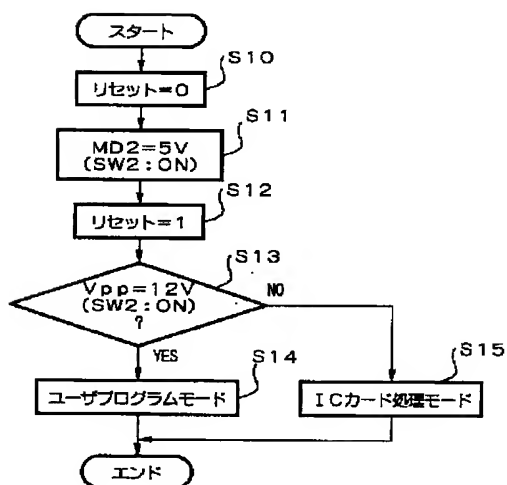
【図2】

第1ブロックB1 (固定)	メインプログラムMP	} SP
第2ブロックB2 (固定)	RAM転送プログラムRP ICカード読取プログラムNP 書き換えプログラムKP	
第3ブロックB3 (書き換え)	ICカード処理プログラムIP	

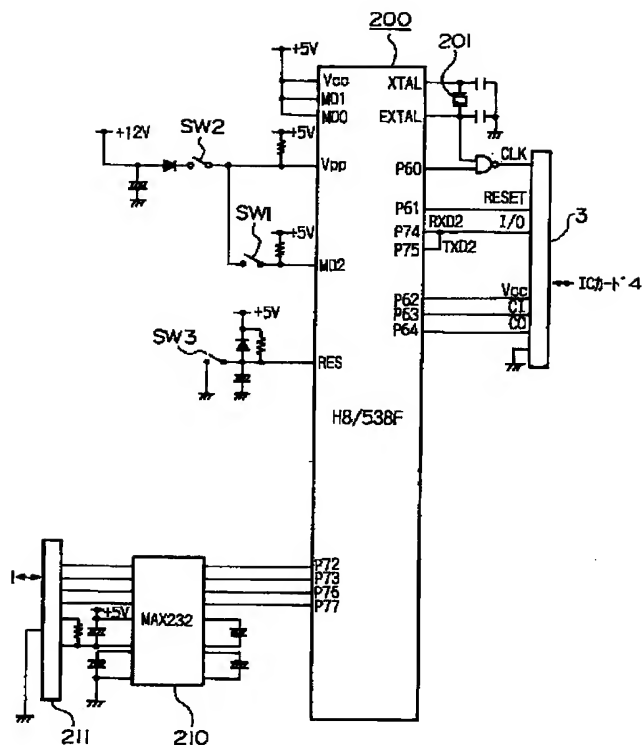
【図10】



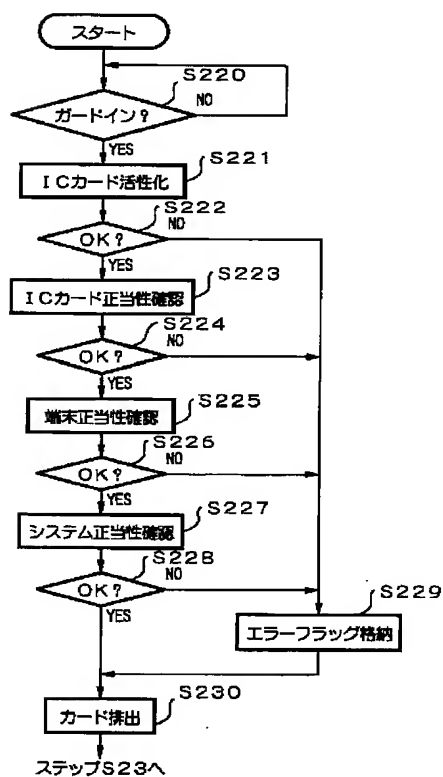
【図5】



【図3】

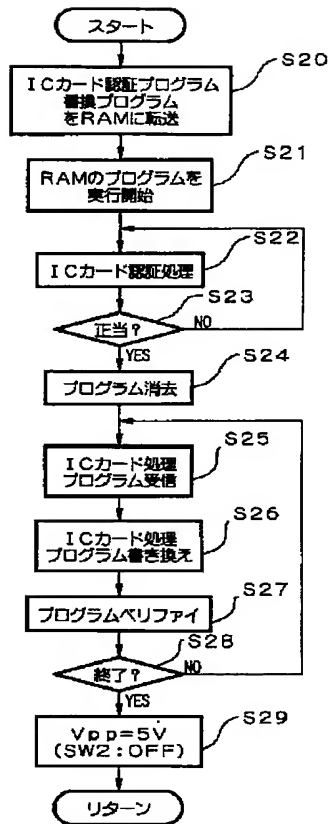


【図7】

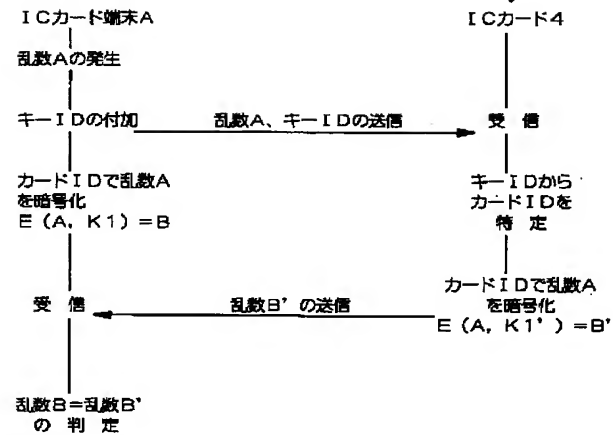


(9)

【図6】



【図8】



【図9】

